CLAIMS

What is claimed is:

1. A method of providing security mechanisms for Internet communications, said communications comprising a plurality of protocol layers including an IP protocol layer and at least one protocol layer above the IP protocol layer; said method comprising:

employing Internet protocol security (IPSEC) authentication header (AH) methodology to derive a plurality of control messages;

utilizing said control messages in a transport mode to provide control plane security; and,

providing security mechanisms, wherein said security mechanisms are utilized at one of said at least one protocol layers above the IP protocol layer.

2. The method of claim 1 wherein said Internet communications are chosen from the group consisting of asynchronous transfer mode (ATM), frame relay (FR) networking and a combination of ATM and FR communications.

3. The method of claim 1 wherein said security mechanisms comprise

control plane authentication and data integrity; and,

support services, said support services comprising key exchange and security database management.

4. The method of claim 1 wherein said Internet communications comprise an ATM protocol, said protocol comprising a signaling layer; and,

wherein said security mechanism provides ATM transport mode security by operating at the signaling layer.

5. The method of claim 4 wherein said at least one of said control messages comprises:

a header;

authentication information, said information containing an integrity check value; and,

ATM calling party address.

6. The method of claim 4 wherein said Internet communications occur through a plurality of ATM nodes, said method further comprising:

establishing a Security Policy Database (SPD) at each ATM node, each said SPD containing separate entries for each virtual interface; and

establishing a Security Association Database (SAD) at each ATM node.

7. The method of claim 1 wherein said Internet communications comprise an FR protocol, said protocol comprising a signaling layer; and,

wherein said security mechanism provides FR transport mode security by operating at the signaling layer.

8. The method of claim 7 wherein said at least one of said control messages comprises:

a header;

authentication information, said information containing an integrity check value; and,

calling party address.

9. The method of claim 7 wherein said Internet communications occur through a plurality of FR nodes, said method further comprising:

establishing a Security Policy Database (SPD) at each FR node, each said SPD containing separate entries for each virtual interface; and,

establishing a Security Association Database (SAD) at each FR node.

10. An apparatus for providing security for Internet communications, said communications comprising a plurality of protocol layers including an IP protocol layer and at least one protocol layer above the IP protocol layer; said apparatus comprising:

at least one control message derivation module for deriving for said communications a plurality of control messages utilizing Internet protocol security (IPSEC) authentication header (AH) methodology;

a control plane security module for utilizing said control messages in a transport mode at one of said at least one protocol layers above the IP protocol layer.

11. The apparatus of claim 10 wherein said protocol layers comprise a signaling layer and said control plane security module operates at the signaling layer.

12. The apparatus of claim 10 wherein said Internet communications are chosen from the group consisting of asynchronous transfer mode (ATM), frame relay (FR) networking and a combination of ATM and FR communications.

13. The apparatus of claim 12 wherein at least one of said plurality of control messages comprises:

a header;

authentication information, said information containing an integrity check value; and,

ATM calling party address.

14. An apparatus for providing control plane security for Internet communications, said Internet communications comprising a signaling layer and occurring over a network communication system comprising a User-Network Interface (UNI) state machine and a Private Network-Network Interface (PNNI) state machine, said apparatus comprising:

a signaling state machine (SSM) employed as a shim layer protocol, wherein said SSM performs the following functions:

in a case of a user incoming message, it passes an authenticated message to the signaling layer or terminates the message;

in a case of a user outgoing message, it computes a message digest for the message it receives from the signaling layer, creates an Authentication Information Element (AIE) and appends the AIE to the message;

in a case of a network incoming message, it forwards an authenticated message or terminates the message; and,

in a case of a network outgoing message, it forwards the message.

15. The apparatus of claim 14 in which SSM further comprises a key management component.

16. The apparatus of claim 15 in which said Internet communications is selected for the group consisting of asynchronous transfer mode (ATM), frame relay (FR) networking and a combination of ATM and FR communications.

17. The apparatus of claim 15 in which said Internet communications comprises FR communications and said SSM comprises a Management Information Base (MIB) management component.